

**Notice of Allowability**

Application No.

10/633,907

Examiner

Fritz Alphonse

Applicant(s)

SZOR, PETER

Art Unit

2112

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the amendment filed on 5/21/2007.
2. ☒ The allowed claim(s) is/are 1,2,5-18 and 20.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All b) ☐ Some\* c) ☐ None of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 5/22/2007
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date \_\_\_\_\_
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

  
GUY LAMARRE  
PRIMARY EXAMINER

### **DETAILED ACTION**

0.1 This office action is in response to the amendment filed on 5/21//2007. Claims 1-2, 4-18 and 20 are amended. Claims 3 and 19 are canceled.

### **EXAMINER'S AMENDMENT**

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with the Applicant's Representative, Lisa A. Norris on 9/4/2007.

The application has been amended as follows:

Claim 17: line 2, after computer-readable medium replace "containing" by ---storing---.

Claim 20: line 20, after computer-readable medium replace "containing" by ---storing---.

### ***Allowable Subject Matter***

2. After further search and through examination of the present application and in view of the prior art of record, claims 1-2, 4-18 and 20 are found to be in condition for allowance.

### ***Reason for Allowance***

3. The following is an examiner's statement of reasons for allowance: The present invention relates to detection and prevention of malicious code propagation, such as computer worm propagation.

To achieve the inventive goal, independent claims 1 and 17 identifies the distinct features "wherein upon a determination that the request is not suspicious, releasing the request; and

Art Unit: 2112

wherein upon a determination that the request is suspicious, adding a request entry to a request database, the request entry identifying the request, generating a counter value associated with the request entry, determining whether the counter value meets a counter value threshold, and wherein upon a determination that the counter value meets the counter value threshold, determining that malicious code activity is detected.”

Independent claim 5 identifies the distinct features “wherein upon a determination that the request is suspicious, adding a request entry representative of the request to a request database, and determining whether malicious code activity is detected on the host computer system based upon the request entry; and wherein upon a determination that malicious code activity is detected on the host computer system, generating a notification that malicious code activity is detected on the host computer system, and implementing one or more protective actions.”

Independent claim 7 identifies the distinct features “determining whether malicious code activity is detected on the host computer system based upon the request entry, wherein the determining whether malicious code activity is detected on the host computer system based upon the request entry further comprises: generating a counter value associated with the request entry; and determining whether the counter value meets a counter value threshold, wherein upon a determination that the counter value does not meet the counter value threshold, determining that malicious code activity is not detected on the host computer system, and wherein upon a determination that the counter value meets: the counter value threshold, determining that malicious code activity is detected on the host computer system.”

Independent claim 12 identifies the distinct features “an analyzer module coupled to the intercept module, the analyzer module for determining whether the request is suspicious utilizing at least a standards list, the analyzer module further for adding a request entry corresponding to the request to a request database when the request is determined as suspicious, the analyzer module further for determining whether malicious activity is detected on the host computer system based on whether a counter value associated with a request entry meets a counter value threshold.”

Independent claim 20 identifies the distinct features “determining whether the request is suspicious, wherein upon a determination that the request is suspicious, adding a request entry representative of the request to a request database, and determining whether malicious code activity is detected on the host computer system based upon the request entry; and wherein upon a determination that malicious code activity is detected on the host computer system generating a notification that malicious code activity is detected on the host computer system, and implementing one or more protective actions.”

4. The first cited reference Chesla (US Pub. No. 20040250124 A1) discloses method and apparatus for protecting networks from malicious traffic. The second cited reference Pak et al. (U.S. Pat. No. 7,080,408) discloses a system, method and computer program product provided for network-base scanning for malicious content.

However, the features recited in claims 1, 5, 7, 12, 17 and 20 in the instant application (No. 10/633,907) are neither anticipated nor render obvious by Chelsea and Pack references nor any other prior art of record.

These limitations specifically mentioned above in conjunction with all other limitations of the base claims 1, 5, 7, 12, 17 and 20 would not have been obvious over, would not have been fairly suggested by the prior art of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

### ***Conclusion***

5. Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C. 20231

**or faxed to:** (703) 872-9306 for all formal communications.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fritz Alphonse, whose telephone number is (571) 272-3813. The examiner can normally be reached on M-F, 8:30-6:00, Alt. Mondays off.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques, can be reached at (571) 272-6962.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (571) 272-3824

Information regarding the status of an application may also be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

Art Unit: 2112


system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Fritz Alphonse

Art Unit 2112

September 12, 2007



GUY LAMARRE  
PRIMARY EXAMINER